Privacy Implications of Context-Aware Services

Were Oyomno
Lappeenranta University of Technology
P.O.Box 20, 53851,
Lappeenranta, Finland
were.oyomno@lut.fi

Pekka Jäppinen
Lappeenranta University of Technology
P.O.Box 20, 53851,
Lappeenranta, Finland
pekka.jappinen@lut.fi

Esa Kerttula
Lappeenranta University of Technology
P.O.Box 20, 53851,
Lappeenranta, Finland
esa.kerttula@lut.fi

ABSTRACT

Personal information handling in current and anticipated context use cases is worrisome. This notwithstanding, contextual services are rapidly proliferating into most niches of society, catalysed by technological advancements in sensing, ubiquity and mobile computing. Evolving social trends, catastrophic events and the economics of personal information further escalate the frenzy. Consequently, contextual applications have propagated into personal, community, government and corporate services. Unfortunately, these services are seldom developed with onset personal information leak concerns. As a result, personal information pieces often leak in their handling, eroding the users' privacy. Privacy erosion is attributed to information leaks through covert acquisitions and re-purposing of legitimate data. Privacy loss from such erosion exposes individuals to significant harm often intractable or costly. This study identifies and sensitises information handling vulnerabilities on their privacy implications in context-aware services. We assert the need for stakeholders in contextual services to deliberate privacy implications of context throughout its life cycle as opposed to, detached focus at collection, transmission or usage points. Notably, privacy threats will intensify as computing further invades the sacred precincts of our private, public and domestic lives.

Categories and Subject Descriptors

J.7 [**Computer Applications**]: Computers In other Systems—*command and control, consumer products, real time*; K.4.1 [**Computers and Society**]: Public Policy Issues—*abuse and crime involving computers, ethics, privacy, transborder data flow, use/abuse of power*; K.6.5 [**Management of Computing and Information**]: Security and Protection—*authentication, invasive software, unauthorised access*

General Terms

Design, reliability, security

COMSWARE '09 June 16-19 Dublin, Ireland

Keywords

Context-Aware, Personal information, Privacy, Anonymity

1. INTRODUCTION

The rapid development of mobile communications and terminals provides new opportunities for the creation of wireless and mobile applications. The ever-growing amount of mobile devices is increasingly affecting services and service use. Customers are no longer tied to specific locations but rather can access and use the same range of services while moving. Small locally accessible services are taking their place alongside the globally accessible Internet services. These local services will be accessed via small mobile devices with a growing variety of capabilities.

Due to the limited user interfaces on these devices, the usability of service needs to be enhanced through automation and adaptation of the service behaviour for a given situation. Since the customers are not tied to a particular location, the situation and surrounding conditions can be different for separate service uses or can even change during the service use.

For accurate adaptation the service would require more and more information about the surrounding conditions i.e. information about the given context. These context-aware services will weave into our everyday lives and through automation a lot more additional information is transmitted without explicit user consent.

When the services require more and more information about customer and customer context, it raises a question of how all this would affect customer privacy. Most of the context information is readily available for the services. Thus, not much effort has been put forth to protect such *"harmless data"* from leaking. While protecting a lone piece of context information may feel as a waste of resources, a combination of these contexts with associated user identity and the knowledge of the used service may pose threat towards privacy.

This paper considers different possible intrusions on privacy and the underlying factors that make them possible. We begin by outlining scenarios where context information is used in Section 2. Section 3 provides an overview context usage by describing the life cycle of context information and Section 4 exposes context leaks, vulnerable points and their privacy risks. Section 5 discusses the privacy implications before concluding the study.

Digital Object Identifier: 10.4108/ICST.COMSWARE2009.6545
http://dx.doi.org/10.4108/ICST.COMSWARE2009.6545

2. CONTEXT USE CASES

Dey's [1] and Chen's [2] definition of context information have been extensively referenced by scholars. We define context broadly to encompass any enriching information about an entity's prevailing situation, including but not limited to its interactions, attributes and changes to these. In this study, context information entails, prevailing identities, current activity, specific roles, allocated credentials, preferences, position/location, proximity, calendar scheduled activities, device profiles, service use histories and sensory data [1, 2, 3]. Accordingly, contextual services adapt their functionality to current context [4].

Context information is used in two dominant ways: service facilitation and service enhancement. In service facilitation, no context implies no service; an Internet based employment agency requires information regarding job seekers (e.g. names, qualifications, experience) and potential employers (e.g. salary, benefits, job descriptions) to provide the service. In contrast, for service enhancement information is a necessary but, insufficient condition to provide the service. A hotel recommender system still recommends hotels without the users' contexts. However, by supplying budget, location and other details, the recommended hotels closely match the users' preferences. Evidently, context information used in service facilitation is more personal identifiable vis-à-vis service enhancement [5].

The popularity of mobile computing, advancements in sensing technology, declining sensor costs, and increasing benefits of personalisation are escalating context-awareness into society. Consequently, technology is continuously in touch with most parts of our lives, availing and optimising mechanisms to collect, aggregate, reproduce, manipulate, process and analyse situations. Contextual applications are increasingly valuable in assisting people living with various disabilities (e.g. elderly, handicapped and invalids), healthcare monitors and fitness trainers [4].

Organisations increasingly realise and anticipate value in personal information collection and context exploitation to warrant changes in business models [4, 6]. Public sector institutions derive efficacies from: electronic payments and ticketing [7], service directories [8], guidance systems [9] and, tracking and surveillance [10, 11]. Rapidly, contextual-services are occupying three *'isolated'* service spheres of society:

1. Individual/community services
2. Government services
3. Corporate services

2.1 Individual/community services

Individual spheres encompass our solitude confines like homes and offices, while the confines shared with society members we identify with are public community spheres e.g. malls, streets, church, libraries and schools.

Individual spheres embody digitally enhanced environments e.g. aware homes, smart/sentient offices and active spaces, composed of systems surrounding, pervading and intelligently serving occupants pleasantly and unobtrusively [12]. European Union's initiative of disappearing computing recognises their significance in assisted home living for elderly and invalid citizens on daily routines [4]. User empowerment, user friendliness and support for human computer interactions by individual services are hinged on a mobile identity that can be tracked, surveilled and monitored within the environment in service provision.

Digital intelligence is rising in community spheres, particularly urban landscapes where majority of world populations reside. Urban landscapes and societies are continuously evolving in practices, behaviours and routines. The evolutionary complexity increasingly demands participants in urban society's daily life to trade some personal information for administration (e.g. drivers license), benefits (e.g. loyalty cards) or service (e.g. E-shops). Accordingly, most urbanites have digital means (e.g. handhelds, biometric passports, bus/train tags) to automate the trade and access personalised services [13, 14, 15, 16]. In such landscapes, contextual services roles are focused on eliminating seams between services (e.g. bus and train ticketing) and address inefficiencies of interactions among urbanites, accessibility to location/environment information and services, and ease landscape navigation [17, 18].

Individual and community services are complex regardless of their popularity. Complexities arise from ownership of sensors and data concerns i.e. placing sensors in malls requires approval of many stakeholders. Additionally, entities have multiple identities, everchanging tastes, constantly enter, leave and use services with varying statistical densities of unpredictable patterns between times, days and seasons.

2.2 Government services

Public services providers of health, national security, emergency response and law enforcement are constantly pressured to improve their processes and lower operational costs. These compel them to improve their information handling in minimising duplicate processes, response time and improve decision making. A number of these providers are seeking refuge in context-awareness e.g. healthcare and policing services.

Contextual services are revolutionising the healthcare and medical industries. New instrumentation ease and facilitate the collection of vast amounts of medical records, prescription histories and payment trails for larger populations over longer time periods. This information is aggregated and correlated, generating even more data about individuals that were previously unattainable. The revelations are relationships and predictions between ailments and other factors to assess treatment efficacies, maintain epidemics, detect diseases early and effectively personalise treatments. Systems monitoring patients vitals are remotely and automatically accessible, providing access to medical expertise to distant and remote patients (e.g. tele-cardiology, tele-radiology, and tele-psychology) [19]. Wearable healthcare assistants sense pulse waves, user's actions and postures, capture contextual photos and continuous voice [20]. Adherence to medical prescriptions are ubiquitously monitored and electronic patient record systems [21] presents physicians with relevant medical records automatically.

This evolution of healthcare blurs the distinctions between the practice, science, businesses and regulation of medicine. New model of healthcare strives towards more sharing of patients information to support the continuity of care maintained from one specialists to another. Pharmaceuticals, insurance and medical researcher are positioned adjacent to healthcare industries sharing sensitive information pieces. Mobile terminals, fitness accessories and healthcare moni-

Digital Object Identifier: 10.4108/ICST.COMSWARE2009.6545
http://dx.doi.org/10.4108/ICST.COMSWARE2009.6545

tors manufactures are converging to integrate wares enabling interoperability [10, 22].

Security and law-enforcers are integrating biometrics and deoxyribonucleic acid into identities. Combined with contextual applications, surveillance deployments e.g. video surveillance are much cheaper to deploying than human officers. Situations become easily observed, individuals identified faster, more accurately and less expensively. This means that criminals can also be arrested for wrong doing in the past not just the present.

Implantable RFID tags are useful in identification of newborns in hospitals, abducted children, lost Alzheimers' patients and incapacitated individuals. Tags facilitate fast and automatic access to medical records, treatment histories or known allergies of an incapacitated victim. Proving valuable to emergency and medical personnel in their efforts to save lives. This is because the probability of separation or damage is lower that of medical bracelets, military tags, medical cards and handhelds while providing relevant data timely [6].

2.3 Corporate services

Private sector corporations in finance, marketing and research have a history of using client information. The information improves processes, increases profitability and creates new revenue streams. Mining this data, has facilitated categorises, profiles and credentials validation. Evidence of value placed on consumers information are seen in its comodification as enterprises spend generously for its collection, aggregation, verification, storage and analysis. Typical corporations profiting from personal information include advertisement, employment and data aggregators who repackage already available personal data from many sources (e.g. credit validators) [23].

Business models have adapted to context in service provision and value addition. Enterprises retailing goods and services tailor and target their products to client's unique tastes using contextual services. Customisation increases client retention, repeat visits, profit margins and quality data. Products are offered more to audiences, most likely to purchase them and services are more dependent on preferences, habits, purchase histories, profiles and contacts. Not-for-profit, charity and non-governmental organisations are becoming increasingly sophisticated in their gathering of information about contributors, members and potential contributors. They often employ similar techniques to profit organisations, and thus have more or less similar information (e.g. donors' credit card numbers to ease future contributions and wealthy clients list).

In anticipation of future use cases, firms gather detailed consumer data extensively. For instance the digital rights management technologies initially developed to deter illegal distribution of copyrighted digital media. However, its current profitably are in the details of consumer behaviours and charging fees on services involved with accessing protected materials e.g. printing [6]. Real-time enterprises leveraged contextual services, to provide immediate access to comprehensive and up-to-date information on processes and procedures. These services prove vital to firms requiring details gathered efficiently, in near real-time stockings of products and market responses i.e. RFID tags and supply chains management. Context also aids in the prevention, detection and recovery of stolen or counterfeit products [24, 25].

2.4 Future scenarios

Demands for seamless and highly customised services will most likely increase as technology matures. Similarly the previously *'isolated'* service spheres will overlap as context information is reproduced, shared, aggregated, integrated and distributed. Wireless World Research Forum (WWRF) has been pivotal in shaping discussions concerning future scenarios. They anticipate service use cases from a ubiquitous perspective and model vignetted scenarios to stimulate discussion as illustrated by scenarios 1 and 2.

Scenario 1 - *"Sabine takes out her mobile personal device which has automatically detected that she has entered the train and therefore asks her whether she would like to find a free seat - and what criteria for this seat should be. Normally, Sabine would ask for seat next to a friend - if any friends were travelling on the train and if such a seat were available. The she would automatically make reservations for such a seat and this would be indicated at the seat so that others were unable to take it. However today, she chooses to find a seat alone in the working section of the train".*

Scenario 2 - *"Five hundred metres from home, Sabine's car communication system queries her for desired preferences on entering the house. She selects her personal profile in terms of house temperature, lighting and music. Today she wants to listen to a band that one of her colleagues plays in. She received the music on her smartphone earlier and now transfers the music to her personal information base so that she can listen to it when she gets in. She gives instructions for this using eye-tracking device and her voice - depending on the traffic and the task she is to carry out".*

Sabine contextually interacts with the environment, shaping services and functionalities to her profile. Sitting criteria, interactions, home environment and played music are transparently influenced by her context. Similar interlaced services are anticipated, rendering the properties of context and its lifecycle imperative for its exploitation by services.

3. CONTEXT AND ITS LIFECYCLE

Context has a distinct lifecycle traceable in services at four core stages: its source, its interpretation, its processing and its usage [26, 27]. Facilitating this flow are interaction mechanisms and repositories. Listed and depicted in Figure 1 are the lifecycle stages.

1. Context Sources (CS) - Mobile terminals internal and external information and sensory hardware e.g. GPS, thermometer, accelerometer, timers, Bluetooth, user profiles, calendar, cellular networks and other devices (Figure 1:①).

2. Context Interpreter (CI) - Processes low-level measurement data from CSs into user abstractions e.g. $(-5^oC \mapsto cold$. Interpretations subjectively vary across individuals, situations and environment (Figure 1:②).

3. Interaction Modes (IM) - Referred elsewhere as Context Exchange Protocols (CEP) [28] facilitate context exchange across entities. Often ubiquitous e.g. Bluetooth, Wireless Local Area Network (WLAN), Infrared and RFID (Figure 1:③).

4. Context consumers (CC) - This environmental-oriented, non-mobile component is associated with sets of services depending on the domains need. It collects, stores

Digital Object Identifier: 10.4108/ICST.COMSWARE2009.6545
http://dx.doi.org/10.4108/ICST.COMSWARE2009.6545

and provides services to subscribers e.g. Sabine's home's personal information base (Figure 1:④).

5. Reasoning Unit (RU) - Decision making realisation of a context-aware application, concerned with context-based reasoning, prediction and analysis. It dictates higher level service adaptability (Figure 1:⑤).

6. Acting Unit (AU) - Perceived service resulting from context utilisation e.g. adjusting house temperature, dimming lights, playing preferred music or reserving seat (Figure 1:⑥ and ⑦).

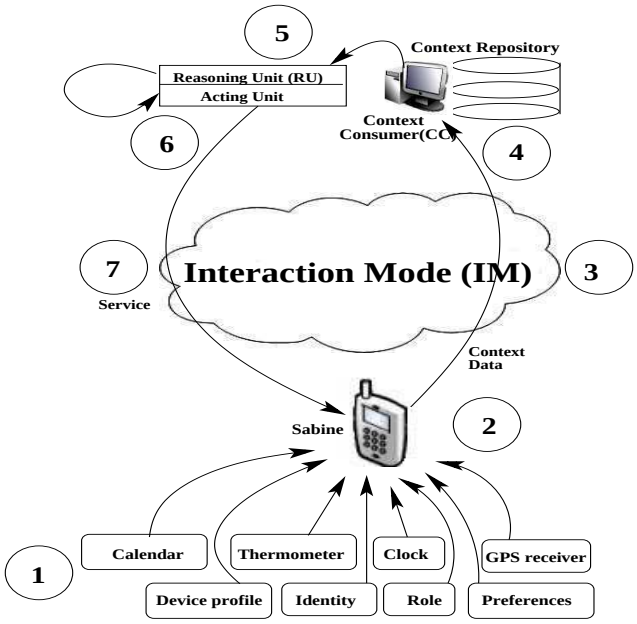

Figure 1: Stages in context-aware system

Figure 1 simplifies contextual services to eight CSs, a single interaction mode and clear distinctions between interpretation, reasoning and actuation. While this supports the context tracing efforts, in reality, responsibilities are rarely well distinguished. Additionally, mobile terminals may store and process context locally. CSs often are heterogeneous and IMs could be frequently interchanged within a single session. This necessitates context handling filters through the following activities [27]:

List 1 Context handling activities.

```
1. Acquisition
2. Representation
3. Interpretation
4. Transmission
5. Utilisation
```

3.1 Context acquisition

Context acquisition entails the accumulation of raw measurement data (voltage levels or symbols), from CSs internal or external to the device to a central location as depicted in Figure 1:①-②. Resulting from differences in manufactures encodings, accuracy and formatting heterogeneities are inherently common in the context acquisition stage. Beyond the encoding and formatting heterogeneities, inconsistencies are also present in sensor querying protocols. Typical protocols include pull-based ①, push-based ② and event-based ③ as depicted in Figure 2. Differences in capabilities and

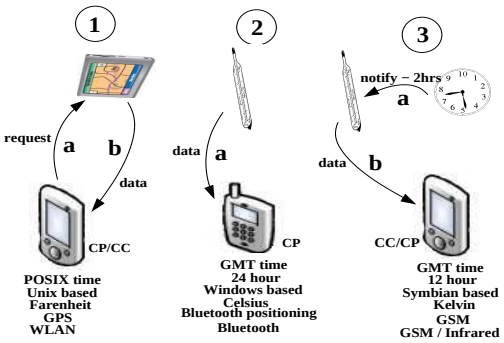

Figure 2: Acquisition and heterogeneity of context

encodings of time (24hours, 12hours, POSIX time or Greenwich Mean Time (GMT)), temperature (Fahrenheit, Celsius and Kelvin scales), location (GPS, Bluetooth or GSM coordinates) and interactions (WLAN, Bluetooth, GSM) are also depicted in Figure 2. This calls for conversion to uniform standards.

3.2 Context representation

In this stage, heterogeneous raw sensory measurements are converted and formatted to low-level context data. Representation activities may include averaging values, smoothing edges, converting to standard formats, adjusting accuracy levels and aggregations.

Representations have evolved from traditional single level to multilevel hierarchical representations. Traditional single level representations focussed on individuals and their interactions with the environment, portraying context data as single level event e.g. changes in location ($\triangle location$), time ($\triangle time$) or temperature ($\triangle temp$). This limited single level representations to static context interactions. However, by saturating context to dynamic artefacts viewable in narrow time frames within a time period, an interaction session or a local influence overcomes this limitations. Beyond this, modern representations have converged towards multilevel hierarchical representation of situation at different abstract levels or complete context representations including dynamic runtime information, human physical and mental state and the static environment [29].

3.3 Interpretation

Context interpretations differ across individuals, times, locations, seasons and situations. For instance, Sabine may considers -5^oC to be chilly in winter, and yet regard the same temperature cold at different time or season e.g. summer. Similarly, this will be mirrored with individual's preferred responses to interpretations. Additionally, previous values or history also affects interpretations. If two hours ago, the temperature was either -21^oC or $+21^oC$, a current temperature of -5^oC will be interpreted differently in both

Digital Object Identifier: 10.4108/ICST.COMSWARE2009.6545
http://dx.doi.org/10.4108/ICST.COMSWARE2009.6545

cases. The importance of context interpretation is to facilitate specific adaptation, customised services able to predict intentions, minimise uncertainty and offer intelligent services [30].

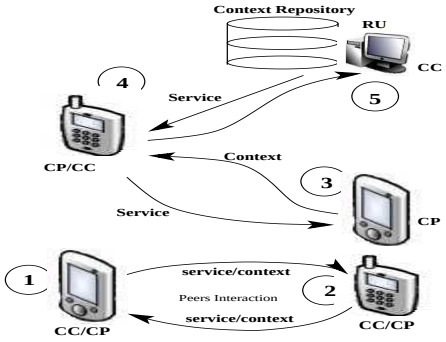

Figure 3: Cooperative context scenarios

Notably, context processing may also occur locally as depicted in Figure 4:(Sabine-2), transmitting rather its higher-level meaning (chilly, in-train, at-home). Unfortunately, local processing tends to be battery and memory intensive, despite optimising bandwidth usage and reducing context consumers processing tasks. This renders it a common approach to transmit low-level context to the consumer node for processing i.e. Figure 4:(Sabine-1). Expectantly, third party context processing co-operations are viable models, particularly, for terminals lacking the capability or in distress (e.g. low battery) as depicted in Figure 3.

3.4 Transmission

Once acquired and represented in palatable form, and modified by user actions for censorship and preference settings, the context is transmitted to the context consumer for interpretation and processing. Transmission means are often ubiquitous as illustrated in Figure 4, with Ad-hoc, Peer-To-Peer (P2P) and Personal Area Networks (PAN) representing typical interaction topologies.

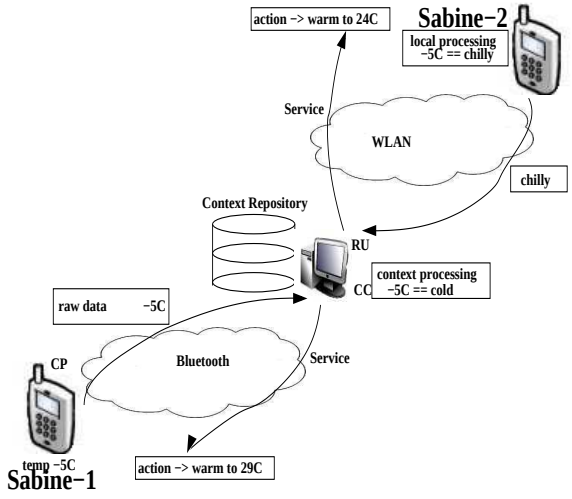

Figure 4: Context interpretation and transmission

3.5 Context utilisation

High-level context is utilised by transforming it into events delivered to an event handler to which context-aware applications subscribe [27].

The RU determines the mode of action, while the actual execution of events is carried out by the AU. Figure 4 depicts Sabine's chilly or cold context transformed to a service used to adapt her environment. Warm the premises to 24^oC. RU decides the probable action is warming and actuation is switching the heaters on.

4. PRIVACY CONCERNS

Demands for better services will be attained by individuals trading more *"harmless data"* about their situations. Currently, most of our daily activities, like eating at restaurant, boarding a train and making a phone call, already generate detailed records that could summarily be described as our *digital shadow*. This shadow provides a view into a persons activities revealing interests, tastes and routines that will be increasingly private and accessible to services. This demands users' to trust the providers to appropriately handle their data.

Nevertheless, initially *'isolated'* service domains e.g. healthcare, insurance, pharmaceutical, banking, law-enforcement and education are integrating, sharing and cross-referencing personal information to provide seamless and efficient services [31]. These domains are also using third parties to aggregate, verify and collect more information on their behalves. This is bound to raise scepticism as domains are bound by different ethics, laws and regulations regarding information use. Significantly, the Hippocratic Oath and informed consent in medicine diminishes as adjacent firms acquire individuals medical information, escalating privacy concerns.

In this study, privacy is focussed on information flow as opposed to physical privacy. Consequently, Westin's [32] definition is appropriate: "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Specifically, we place emphasis on solitude (freedom from observation or surveillance), anonymity (freedom from being identified in public) and reservation (freedom to withdraw from communication).

Services privacy concerns are amplified as sensitive information previously obscured by spatial properties or passage of time become easy to acquire. This is attributed also to societal transformations in their privacy expectations, e.g. criminal records and identities of sex offenders are now public information. Furthermore, post 9/11 governments are demanding more permanent and personal identifiable information from citizens, foreigners and organisations. In certain instances stealth acquisitions without consent, in the interest of national security have been legalised [31]. The totality is sensitive information individuals would prefer kept private, such as location history, are easily inferred. Location history is revealed by trailing service accesses for different services e.g. entry and exit train stations, preferred shopping malls, music and restaurants.

Surprisingly, services are yet to employ adequate privacy preservation mechanisms in the handling of acquired context. Despite scrutiny of the lifecycle, revealing channels of flows could be easily compromised. Typical justifica-

Digital Object Identifier: 10.4108/ICST.COMSWARE2009.6545
http://dx.doi.org/10.4108/ICST.COMSWARE2009.6545

tions to privacy inconsideration are: harmless data, tradeoffs with processing, bandwidth and interoperability. Potentially these threaten to erode users' privacy, exposing them to falsifications, misrepresentations, identity thefts, surveillance, physical privacy violations, financial theft, profiling and ridicule risks. Privacy erosion, by services has been duly noted by adversaries, especially as the costs of compromising techniques and tools decline. Vulnerabilities of context management follow from List 1.

4.1 Acquiring vulnerabilities

Mobile terminals are increasingly able to acquire and utilise context from multiple sources. Lists of pervading services, GPS coordinates from nearby devices and hotspots are potential sources. Users profiles, calendars and meetings are also utilised by contextual services in determining acceptable adaptations. These acquisitions require protocols to facilitate the exchange as well as determine device capabilities and encodings. Credentials have also become increasingly inherent in acquisitions and service provision. In acquisitions credentials permit associations with device or user specific information. Storing this information allows detection repeat visits thereby optimising the acquisitions.

Accessing sensory audit and storage records reveals fine grained history of acquisitions that infers more identifying information, cross-referencing this data thus becomes more revealing. Acquisitions sources and context enquirers rarely are validated or authenticated permitting them to mislead the context-aware system.

4.2 Representation vulnerabilities

Inter-operability of context advocates for standardised representations and storing, and shying away from encrypted transmission and repositories. For instance, calendar schedules, contact list, meeting, virtual business cards and profile settings are often unencrypted in terminals to facilitate cross vendor transaction. These threaten to compromise hosts privacy and anonymity if services can easily understand and access them in their interaction or service provision. Mobile terminals representing the sensed context or situations in easily accessible and comprehensible formats risk compromising the host's privacy.

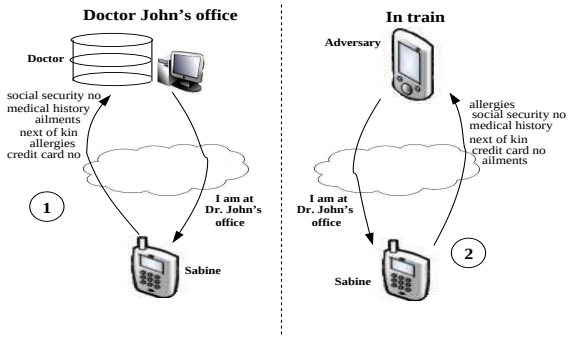

Figure 5: Privacy erosion by sensing

Malicious services able to falsify environmental context to Sabine's device could access private information, such as preferred music, health records and security numbers stored in the device. Figure 5 illustrates an extreme scenario where, sensitive data leaks from Sabine's terminal by falsifying physician's office context. Such vulnerabilities could be exploited by malicious services of employers and insurance screenings. Similar consequences are in issuing incorrect GPS coordinates to drivers' navigation systems, misleading them to wrong destinations. A contextually secured device that lowers its security policy on sensing safe environment, e.g. home, could also be compromised if it acquires falsified home context. More realistic examples are evident in services that intentionally or mistakenly update users device profiles, resulting in them missing important calls or reminders.

4.3 Interpretation vulnerabilities

Contextual service often interpret users situation in formats they can easily understand and modify e.g. in-train, at-mall or with-mike. Justifications for user friendly interpretations are based on interoperability and support for human interactivity. However, these interpretations tend to be privacy vulnerabilities, especially, if they are easily accessible to other services or persons. Accessing context interpretations covertly without the user's knowledge or consent enables fine-grained inference of their situations, such as mode of transportation mode, current location and with whom, thus potentially unearthing details people would prefer kept private, like intimate activities, anonymous encounters and discrete associations.

A classical example exists in libraries. These institutions have fiercely advocated and protected the privacy of their patrons for a long time. Privacy enhanced atmosphere are deemed necessary in encouraging patrons to pursue any subject of their interest, be it controversial, unpopular or ideological, without scrutiny of neighbours, friends, employers or governments. Systems threatening this privacy have been avoided, for example recommender-based on individuals borrowing history. However, embedding of RFID tags that represent books details in easily understood formats, such as title and author, are adopted to automate borrowing procedures. While patrons are more willing to borrow sensitive literature as their checkout is entirely handled by a machine, it threaten their privacy by permitting individuals and services to surreptitiously discover patrons reading habits when in close proximity [33].

Analysis of context interpretations reduces the need for access to physical or material body in order to gather information and intelligence about individuals' past, present and future behaviours. For instance, Bluetooth scans can to some extend reveal users products manufacture based on BD_ADDRs.

4.4 Interactions vulnerabilities

Services inadequately protecting interactions with customers expose their information to eavesdroppers. The difficulty of ubiquitous interactions in detecting such passive attacks is well documented and evident in RFID, WLAN and Bluetooth cases [34], [35], [36], [37]. This leak permits eavesdroppers and other malicious services to infer additionally information from soft surveillance. Despite, encrypting interactions, the source and destination addresses in the packet headers are never encrypted, exposing them to data mining. Such data mining can reveal details of communicating devices, peak and off-peak usage patterns, profile devices owners as well as track their movements.

Digital Object Identifier: 10.4108/ICST.COMSWARE2009.6545
http://dx.doi.org/10.4108/ICST.COMSWARE2009.6545

Monitoring communication traffic in residential areas is currently revealing to adversaries, allowing them to formulate other privacy compromises. This probability of success is raised if the identity of devices can be ascertained, with high probability when individuals are at home.

4.5 Utilisation vulnerabilities

Modifying stored context at either the source or destination, affects the integrity of the data which alters resultant service perception. Therefore, services that interact directly with context sources and consumers repositories of real-time services are potential privacy risk. Due to large volumes of personal information stored at these repositories they could not only expose sensitive details of users activities, but also results tampered with misleading the populations or discrediting the service.

Malicious service able to access repositories encrypted or otherwise can render denial of service attacks by making the data format unusable by other services, e.g. by deleting the password field. Cooperative contextual services also risk reversal credibility of trusted and malicious entities in a service, if the cache is accessible to malicious services. Identity thefts are commonly known scenarios where personal information about persons, e.g. social security numbers and credit card numbers, has fallen into the wrong hands. The ChoicePoint case of 2005 that resulted in personal identifiable information of 143,000 individuals being compromised consequentially followed by 800 cases of identity theft and $15 million in repairs [31].

Future context use cases raise privacy scepticism as individuals' information are further dispersed and retrieved from increasing numbers of sources, consumers and third parties. Privacy leaks are inherent as this trend exposes personal information across domains where it is further reproduced, cross-referenced and correlated with other sourced data. However, current services with reasoning and actuating units inadequately securing their mechanisms risk exposing similar private information indirectly to services restrained from it. This information leak tends to be overlooked, especially if service requests are encrypted. Unencrypted service deliveries permit the linking of particular encrypted request with a clear text service.

5. DISCUSSION

Section 4 raised concerns regarding the chain of custody of personal information by services, highlighting every chain-link leak vulnerability. Services with inadequately defined, validated and safeguarded activities risk compromising user's privacy. Notably, privacy concerns arise from specific use of individual's information rather than the fact of how it is collected. Thus, inadequate safeguards expose context to access and inference by malicious services and adversaries. Illegitimately accessed context is usable in ways users may never know, thereby compromising their privacy. Therefore, accountability of possible context access becomes as important as its use. Stakeholders need to address privacy issues against:

1. What information pieces are private and with whom are they associated?
2. From who are private information pieces withheld?
3. What benefits are realised by withholding or not withholding private information and in whose interests are they?

Refraining from untrustworthy services, entities or adversaries may aid in reducing privacy threats. Unfortunately, it is difficult to identify services that may use personal information to harm, discriminate, ridicule or categorise users. Information re-purposing and sharing are often beyond users control once acquired. At the same time, individuals' privacy have to be balanced against the societal goods, e.g. in detecting terrorists or persons with epidemic diseases.

Improper understanding of the chain of custody by contextual stakeholders weakens protection mechanisms that may exist elsewhere in the service. Furthermore, privacy preservation in services remains complex. Trends suggest the services and facilitators will only increase in numbers and sophistication as scenarios illustrate. Unless attention to privacy becomes an onset priority by developers, plenty of funds will be spent on victims' compensation, privacy recovery and public reassurance. Despite this, context-aware privacy issues remain unpopular among scholars.

6. CONCLUSION AND FUTURE WORK

The role of personal information is increasingly dominant in; personal, community, government, and private sector services. The demands for highly personalised and seamlessly enhanced services are met by acquisition of more personal information, aggregating and sharing it across these formally isolated service domains. This reinforces the imbalance of power, disadvantaging individuals in their interactions ensuring maintenance of the power and resource disparity. This disparity is evident in resources that can be brought to bear versus those available to individuals in information gathering and consequent use [31].

Current and future context-aware services reveal vulnerabilities in their handling of individuals' information. The vulnerabilities expose private information to covert acquisitions without the owner's knowledge or consent. Unless mitigated, users will be victims of significant privacy compromises that are intractable, costly to repair and increase reluctance to engage. However, despite users' privacy concerns, there are broad discrepancies between attitudes and actual behaviour toward privacy protection. This is reflected in the low demand for privacy enhancing products, many users are content with default service behaviours, and many dismiss future consequence of revealing personal information for immediate rewards.

This study identified and sensitised information leaks in context-aware services on their privacy implications. Firstly, existing and anticipated use cases are presented in relation to technological advancements and societal trends. Thereafter, context flow, in a service is traced to clarify potential information leak vulnerabilities. Finally, the leak vulnerabilities are highlighted on their privacy implications to service users. Our objective is to stimulate scholars, developers and service providers' attention on context handling beyond a single entity of responsibility and associated privacy implications.

To address raised concerns, we are developing a privacy preserving framework for context-aware infrastructures. This pertains to investigating distributed privacy preservation mechanisms across services and entities to facilitate seamless-

Digital Object Identifier: 10.4108/ICST.COMSWARE2009.6545
http://dx.doi.org/10.4108/ICST.COMSWARE2009.6545

ness without excessive erosion of individual's privacy and anonymity. Based on trust models and privacy preserving context mining, we aim to model the architecture and develop an adaptable privacy preserving system prototype.

7. REFERENCES

[1] Anind K. Dey. Providing architecutural support for building context-aware applications. In *PhD thesis*, Georgia, 2000. Georgia Institute of Technology.

[2] G. Chen and D. Kotz. A survey of context-aware mobile computing research. *Technical Report TR 2000-381, Department of Computer Science, Dartmouth College*, November 2000.

[3] Anind K. Dey. Understanding and using context. In *Personal and ubiquitous computing*, pages 4–7, London, UK, 2001. Springerlink.

[4] Seng Loke. *Context-Aware pervasive systems*, volume 1. Auerbach publications, 1 edition, 2006.

[5] Pekka Jäppinen. *Mobile Electronic Personality*. PhD thesis, Lappeenranta University Of Technology, 2004.

[6] Max Muhlhauser and Iryna Gurevych. *Handbook of research on Ubiquitous computing technology for real time enterpises*, volume 1. Hershey New York, 2008, 1 edition, 2008.

[7] Olaf Diegel, Glen Bright, and Johan Potgieter. Bluetooth ubiquitous networks: seamlessy intergrating humans and machines. *Emarald, Assembly automation*, 24(2):168–176, Febuary 2004.

[8] ESIGN Workshop Expert Group for CEN/ISSS. Protection profile - secure signature-creation devices type1, july 2001, http://www.bsi.bund.de/zertifiz/zert/reporte/pp0004b.pdf. 2007, Accessed 17th July 2008.

[9] Ichiro Satoh. Experience of context-aware services in public spaces. In *ICPS '08: Proceedings of the 5th international conference on Pervasive services*, pages 81–90, New York, NY, USA, 2008. ACM.

[10] Gaetano Borriello, Vince Stanford, Chandra Narayanaswami, and Walter Menning. Pervasive computing in healthcare. *IEEE Computer society*, (7):168–176, 2007.

[11] Joseph Paradiso, Gaetano Borriello, and Paolo Bonato. Implantable electronics. *Pervasive Computing, IEEE*, 7(1):12–13, Jan.-March 2008.

[12] Victoria Haines, Val Mitchell, Catherine Cooper, and Martin Maguire. Probing user values in the home environment within a technology driven smart home project. *Personal Ubiquitous Comput.*, 11(5):349–359, 2007.

[13] Guanhua Yan, Hector D. Flores, Leticia Cuellar, Nicolas Hengartner, Stephan Eidenbenz, and Vincent Vu. Bluetooth worm propagation: mobility pattern matters! In *ASIACCS '07: Proceedings of the 2nd ACM symposium on Information, computer and communications security*, pages 32–44, New York, NY, USA, 2007. ACM.

[14] Ben Wood, Carolina Milanesi, Ann Liang, Hugues De La Vergne, Tuong Huy Nguyen, and Nahoko Mitsuyama. Forecast: Mobile terminals, worldwide, 2000-2009. Technical report, Gatner Research, 2005.

[15] Mobile phone market forecasts. http://www.linuxdevices.com/news/ns5517786818.html. Accessed 24th June 2008.

[16] Mobile terminal market. http://www.windowsfordevices.com/news/ns5566717572.html. Accessed 24th June 2008.

[17] Piotr Adamczyk, Kevin Hamilton, Alan Chamberlain, Steve Benford, Nick Tandavanitj, Amanda Oldroyd, Kate Hartman, Kati London, Sai Sriskandarajah, Eiman Kanjo, Peter Lanshoff, Kaoru Sezaki, Shin'ichi Konomi, Muaz A. Niazi, Hafiz F. Ahmad, Fauzan Mirza, Arshad Ali, George Roussos, Dikaios Papadogkonas, and Mark Levene. Urban computing and mobile devices. *Distributed Systems Online, IEEE*, 8(7):2–2, July 2007.

[18] Tim Kindberg, Matthew Chalmers, and Eric Paulos. Guest editors' introduction: Urban computing. *Pervasive Computing, IEEE*, 6(3):18–20, July-Sept. 2007.

[19] Voskarides S Pattichis MS Istepanian R Schizas CN Pattichis CS, Kyriacou E. Wireless telemedicine systems: an overview. *IEEE Antennas Propag Mag*, 44(2), April 2002.

[20] Upkar Varshney. Pervasive healthcare and wireless health monitoring. *Mob. Netw. Appl.*, 12(2-3):113–127, 2007.

[21] Jesper Kjeldskov and Mikael B. Skov. Exploring context-awareness for ubiquitous computing in the healthcare domain. *Personal Ubiquitous Comput.*, 11(7):549–562, 2007.

[22] Maria Ebling and Mark Corner. A pervasive personal trainer, an electronic leash, a light canvas... *Pervasive Computing, IEEE*, 7(2):10–11, April-June 2008.

[23] Were Oyomno and Pekka Jäppinen. Security and privacy in a ubiquitous information screen. *7th Minema Workshop, WAWC08 confrence.*, (2):133–143, 2008.

[24] David Molnar, Andrea Soppera, and David Wagner. Privacy for rfid through trusted computing. In *WPES '05: Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pages 31–34, New York, NY, USA, 2005. ACM.

[25] David Molnar and David Wagner. Privacy and security in library rfid: issues, practices, and architectures. In *CCS '04: Proceedings of the 11th ACM conference on Computer and communications security*, pages 210–219, New York, NY, USA, 2004. ACM.

[26] Sandra Haseloff Olivier Coutand, SianLun Lau. An approach using memory-based reasoning for determing the behaviour of mobile, location-aware services. *Context-Awareness for proactive systems CAPS 2006*, pages 43–52, June 2006.

[27] Sandra Haseloff Tino Löffler, Stephan Sigg and Klaus David. The quick step to foxtrot. *Context-Awareness for proactive systems CAPS 2006*, pages 112–123, June 2006.

[28] Lakkala H. Context exchange protocol specification, http://www.mupe.net. 2008, Accessed 4th January 2009.

[29] Luo Sun, Peng Dai, Linmi Tao, and Guangyou Xu. A context representation and management mechanism towards ubiquitous intelligence. *Computer and Information Technology, 2008. CIT 2008. 8th IEEE International Conference on*, pages 809–814, July

Digital Object Identifier: 10.4108/ICST.COMSWARE2009.6545
http://dx.doi.org/10.4108/ICST.COMSWARE2009.6545

2008.

[30] Bruno Bouchard, Abdenour Bouzouane, and Sylvain Giroux. A smart home agent for plan recognition. In *AAMAS '06: Proceedings of the fifth international joint conference on Autonomous agents and multiagent systems*, pages 320–322, New York, NY, USA, 2006. ACM.

[31] Anind K. Dey. Engaging privacy and information technology in a digital age. In *National Research Council Of The National Academies*, 500 fifth street, N.W, Washington, DC 2001, 2007. The national academies press.

[32] Alan F. Westin. *Privacy and Freedom*. Number 2. The Bod-ley Head, 1967.

[33] Von James Waldo, Herbert S. Lin, and Lynette I. Miller. *Engaging privacy and information technology in a digital age*, volume 1. Natl Academy Press, 1 edition, 2007.

[34] Frank Stajano. *Security for Ubiquitous Computing*. John Wiley and Sons, February 2002.

[35] Martin Herfurt. trifinite security advisory: Buffer overrun in toshiba bluetooth stack for windows (trsa00001). 20th June 2006.

[36] Collin Mulliner and Martin Herfurt. Blueprinting - remote device identification based on bluetooth fingerprinting techniques. December 2004.

[37] Martin Herfurt. Bluesnarfing cebit 2004 - detecting and attacking bluetooth-enabled cellphones at the hannover fairground. March 2004.

Digital Object Identifier: 10.4108/ICST.COMSWARE2009.6545
http://dx.doi.org/10.4108/ICST.COMSWARE2009.6545